Encryption ethics: are email providers responsible for privacy?

November 28 2013, by Adam Henschke

Protest against NSA surveillance. Credit: Mike Herbst

Ex-National Security Agency (NSA) employee Edward Snowden's various leaks – the most recent being a slide showing that the NSA infected 50,000 of computer networks with remote-controlled spyware – confirm that state intelligence agencies around the world have been collecting and analysing people's behaviour online for years.

Many people now feel that their online privacy and anonymity have been undermined – particularly as major service providers like Google, Facebook and Apple have been compromised. In response, some email service providers (such asYahoo! last week) are now offering full encryption of users' data.

While privacy is generally seen as morally desirable, the ethical issues surrounding encryption technologies require some closer investigation. In order to properly assess such things, we need to assess not just the claims but the moral foundations upon which they are based.

What, then, are the main moral justifications for encryption? What are the arguments against it? And finally, what responsibilities do encryption service providers owe their clients and the public at large?

The case for encryptionThe most obvious case for supporting encryption is one of basic liberties: certain human rights, it might be argued, are fundamental, and privacy is one of these. As such, personal information ought to be respected and kept private. Encryption is simply a method of achieving this goal.

Simply claiming a right, however, is not sufficient justification on its own. As some—such as ethicist Fritz AllhofF—have argued, where there is an immediate danger to an individual's right to physical security, then another's rights might be justifiably waived.

This principle could also apply to the online world. If, for instance, encryption were to allow a cyberattack on the scale of Pearl Harbour to go unchecked – as described in the video below – then perhaps there might be a case for sacrificing some rights to privacy.

Another reason is that government internet surveillance threatens the openness of the internet, undermining the spirit of the internet itself.

According to this view, the principle of the internet beingopen and free should be sacrosanct.

But note that this is more of an ideal than a reality – for instance, the actual code that operates the internet already places limitations upon it. For instance, American law professorLawrence Lessig wrote of code that is designed to facilitate identification online or the rating of content.

Others have concerns over the prospect of information being misused, particularly by police agencies. In response to the platitude "if you have nothing to hide, you have nothing to fear", this argument retorts "if you have something to fear, you have reason to hide".

The use of social media to target people following the Arab Spring is one example of this. Encryption may be permitted in this sort of situation, but this is typically only relevant with regard to states that do not recognise the rule of law.

A final reason is that surveillance can lead to "chilling", where fear of oversight changes behaviour online. Arguably, there might be instances in which something like this might be desired.

For instance, most would agree that production and distribution of child pornography should be limited. Encryption, however, makes these activities easier to get away with. The debate, then, ought to be about what behaviours we chill, how we go about chilling them and what the unwanted side effects—if any—might be.

If we wish to make something illegal, laws need to be very carefully written. Contrary to its legal status, the act of teenagers "sexting" each other does not seem like production and distribution of child pornography.

Furthermore, we need to ask how far the analogy extends – producing and distributing child pornography is not the same as illegally downloading a Miley Cyrus song.

While the child pornography example shows us that some limitation of internet behaviour might justified, it does not necessarily help us in telling what else ought to be limited.

Reasons against encryption

Supporters of encryption may point to the principle of presumption of innocence. After all, if only a small percentage of online activity is of a serious criminal nature, why should all be under surveillance?

There are reasons to treat such reasoning with scepticism. Given that encryption can allow and enable criminal activity—child pornography, drug trafficking, communication within criminal networks and so on—the question is this: if surveillance of criminal activity is permitted or even expected in the physical realm, why not in the virtual?

Encryption, after all, can protect those who attack the security of others.

It is the state's duty to ensure national security. This is an important point – when there is a major terrorist activity, the state is held responsible for not preventing it.

If we demand strong limits on state surveillance, who is responsible for protecting innocents from attack? The point is that we can't expect total freedom and total security.

Where it endangers individual or national security, encryption may well be problematic. Nevertheless, we need to properly interrogate the case for state surveillance as well as the case for private protection.

If the state claims that encryption is contrary to national security, it is required to clarify what "national security" means, how encryption undermines it, and what individual and social goods are being traded against security.

Responsibilities of service providers

If encryption can be justified, what moral responsibility do the service providers have? For instance, do they have a duty to report criminal behaviour? The principle of medical confidentiality has its limits, after all: if a person states that they are planning a crime, or a child shows signs of abuse, there is a responsibility to report this information. Could it be said that encryption service providers are under the same responsibility?

Secondly, should service providers guarantee encryption? The deal made with the service provider gives a user an expectation of encryption, which may in turn encourage certain behaviour. But if encryption is not guaranteed, if there are ways of cracking it, do users have a moral claim against service providers? This is akin to a claim of entrapment.

Finally, the service providers also need to be consistent: if they offer encryption because of moral reasons, then these moral reasons ought to hold the provider to the same standard as the state. For instance, if the claim of a right to privacy holds, then the service provider cannot justifiably monitor the data or metadata or use it to make money, as this would also constitute an invasion of privacy.

This is only a brief overview of the issues at stake, but offers a little insight into the moral tensions involved in offering encryption services.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation

Citation: Encryption ethics: are email providers responsible for privacy? (2013, November 28) retrieved 1 July 2024 from https://phys.org/news/2013-11-encryption-ethics-email-responsible-privacy.html